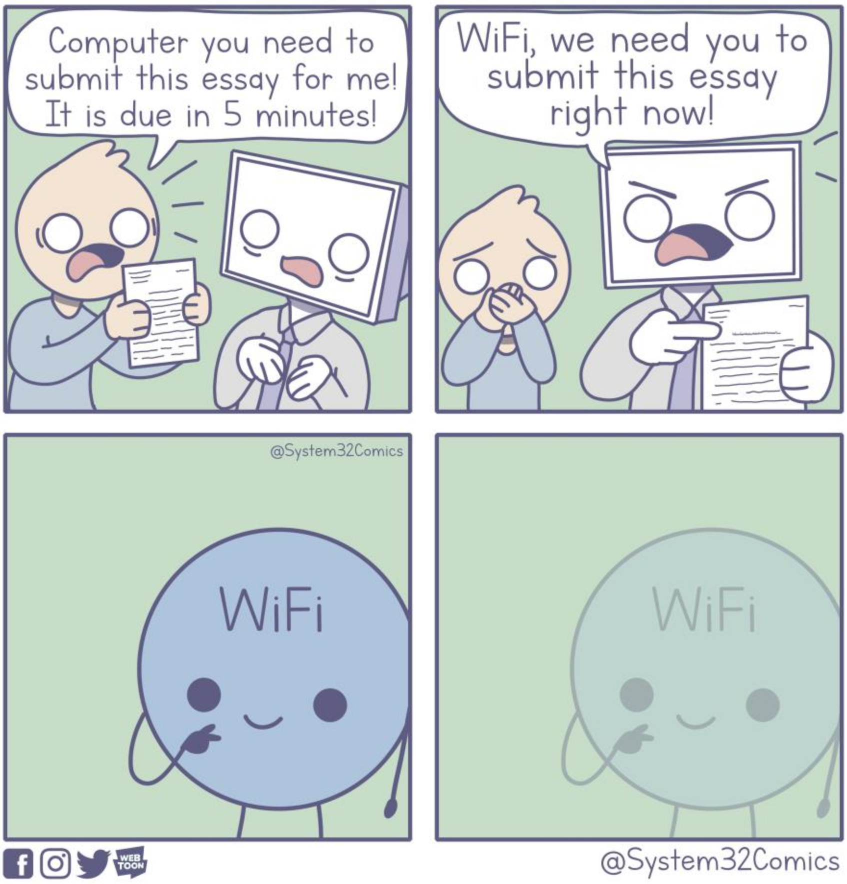

Computer you need to submit this essay for me! It is due in 5 minutes!
WiFi, we need you to submit this essay right now!
@System32Comics
WiFi
WiFi
WEB TOON
@System32Comics

ASSIGNMENT 3

ITRI 625

ENRICO DREYER

31210783

Table of Contents

Introduction

In this assignment we were asked to give our own explanations of the ten commandments of computer ethics, as well as give examples of each and possible improvements or shortcoming. According to Techspirited (2020), the ten commandments are there to give instructions on how to use computers ethically. Computer ethics is a philosophy of ethical values, these values should be adhered by every computer user.

Each commandment is explained in the next part of the paper.

1. Thou shalt not use a computer to harm people

In simple terms a user should not use computers in ways that can harm other people. This is not limited to injury that is physical but includes corrupting or harming other user's data of files. This commandment revolves around users not using a computer to steal other individuals' personal information.

Looking form an ethical perspective destroying or manipulating files of other users are wrong. Writing programs that runs on execution with the intention to steal, gain or copy data that you do not have authorized access to is ethically wrong. Examples include spamming, hacking, phishing, or cyber bulling (Technology, 2014).

2. Thou shalt not interfere with other people's computer work.

In simple terms users should not use computers to cause interference with other computer users. Computer software can cause disturbance in others work. An example of this is viruses that meant to interfere with normal functionality of a computer, harm other useful computer programs, or delete files that are being used on a computer (Stoplearn, 2019).

Different ways that a malicious software can disrupt the functionality includes the overload of computer memory with the use of excessive consumption, thus slowing the actual functionality. Malicious software can also cause a function to act wrongly or cause the function to stop working. The conclusion is that using malicious software to interfere with other people's computer functionality is unethical.

3. Thou shalt not snoop around in other people’s files.

In simple terms users should not use computer software to spy on other people’s data. As people we know that reading other people’s personal messages is wrong. This includes reading someone else’s files, email messages or documents (Stoplearn, 2019).

Obtaining and reading someone else’s data is still breaking into someone’s room and reading their diary. Snooping around in someone else’s personal files and reading the content of those files is considered invasion of privacy.

An example of an exception of this is ethical cyber-crime cases, where intelligence agencies spy on internet activities that are suspicions and have the potential to save someone’s life.

4. Thou shalt not use a computer to steal.

In simple terms people should not use computer technology to steal from other users. This is as good as robbery. This entails leaking or stealing confidential information, for example it is wrong to acquire personal information from an employee database or patient detail from a hospital database.

This is also considered fraud, where a user breaks into a bank account to acquire confidential information about that account or use it to obtain access a different account. Computers can also be used to store the information that was stolen. As no system is fully protected against cyber theft, it makes it exponentially harder to protect sensitive information and there is always going to be someone that is trying to gain access to that system.

5. Thou shalt not use a computer to bear false witness.

In simple terms a user should not use computer technology to spread information that is not correct. The spread of information has become vital in today’s society, this means that the information that is being spread can contain false news or rumours (Wang, 2014).

Information can spread easily through emails or social networks such as Facebook. Anyone can create a post on Facebook without a fact check and being involved in the spread of falsifying information is unethical. Pop-ups or mails are a common method of spreading wrong information and give false warnings in order to sell a product, such as warning a computer user about shoes going up in price as they are running out of stock.

6. Thou shalt not use or copy software for which you have not paid.

In simple terms you should not use computer software that you download or copy without paying for them, with the exception that the software is free to use (Rowenna, 2020). Software is like any other literary or artistic work and is copyrighted. The original code is owned by the person who created it and is copyrighted in their name, unless he works for a company, then the company owns the code and copyright.

The copyright holds true, unless the created announces it as free to use. The conclusion is that using code that is not free to use without paying for it is unethical. An example of this is creating a torrent to give or receive files over the internet in a peer-to-peer manner.

7. Thou shalt not use other people’s computer resources without authorization.

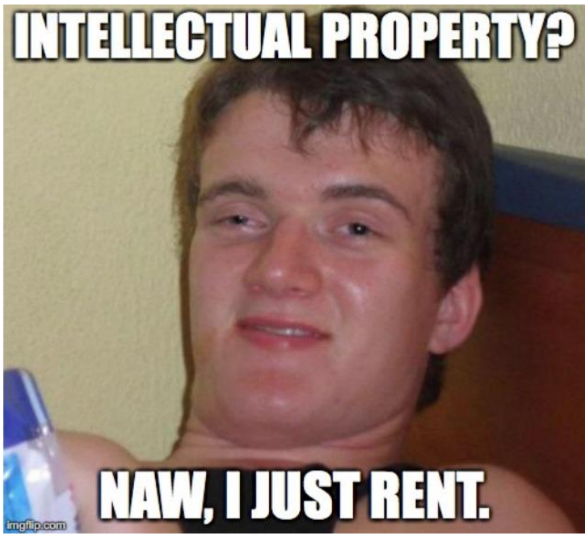
In simple terms a user should not use another computer without authorization from the owner of that computer. Systems that have more than one user use an access control list, where each user has their own password, and their profile is linked to a “role” such as admin. Breaking into the system with someone else’s password, you are intruding their private space and that is unethical.

It is also not ethical to hack or force passwords to gain unauthorized access to a password-protected system. Accessing data that you as person is not allowed access to is unethical and is considered an offence. Improvements include having ACL build into each API call of our system, as well as not using one password for every account and making your password as strong as possible (Upadhyay, 2020).

8. Thou shalt not appropriate other people's intellectual output.

In simple terms it is considered wrong to claim ownership of work that was done by someone else. Each program or piece of code that is written is the developers own property, unless the project is owned by a company then it becomes the company's intellectual property. Thus, coping or using it as your own is considered unethical.

This also applies to any program, creative work, or design. Claiming ownership of work that is not yours in ethically wrong and should not be done. According to Mustapha (2020) to protect yourself against the intellectual property of software you can copyright a file, file a patent, make use of source code licenses or have developers sign an intellectual property assignment agreement.



9. Thou shalt think about the social consequences of the program you write.

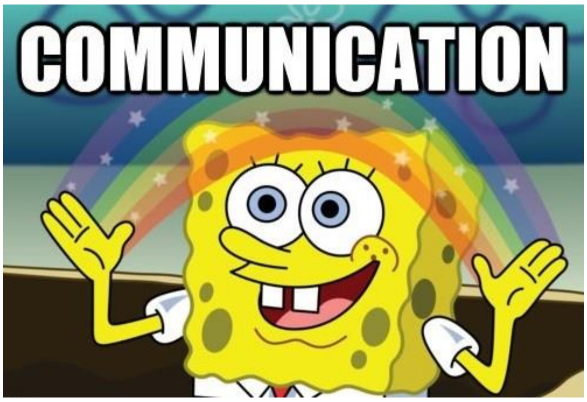
In simple terms before you develop a system or software, you need to think about what impact that software will have. When you think about the social consequences that software can have, describes a wider perspective of looking at computer technology. Software can reach millions of users, an example of this can be video games, educational software, or animations (Stoplearn, 2019).

Designing a video game or animation there must be an understanding on how the targeted audience is. For example, an educational program for kids should not contain content that affects them negatively. In the same light, writing software with malicious intent is ethically wrong. This can be protected against by having software firms and software developers considering their influences of their code on society.

10. Thou shalt use a computer in ways that show consideration and respect.

In simple terms when using computers for communication you need to be courteous and respectful to other users. The same communication etiquette in real life applies to communication that we use over the computer. When talking to each other over the internet, we need to treat each other with respect.

As a user, you should use abusive language, pass irresponsible remarks, not intrude other, invade their privacy, or make false statements. You should be courteous when communicating over the internet and respect others' resources and time and be considerate with new computer users, such as your parents. An improvement to this is to not interact with other users that does not follow the same moral values as you.



Conclusion

Each commandment was explained in simple terms as well as giving some examples of each. The commandments was also viewed in an ethical way.

References

Mustapha, Z. (2020). 4 Ways To Protect The Intellectual Property Of Your Software. https://www.lifehack.org/517592/4-ways-protect-the-intellectual-property-your-software

Rowenna, A. (2020). The Ten Commandments of Computer Ethics. https://remultabentekwatro.wordpress.com/28-2/

Stoplearn. (2019). Ten Commandments of Computer Ethics. https://www.stoplearn.com/ten-commandments-of-computer-ethics/

Technology. (2014). 10 commandments of computer ethics with example. https://www.slideshare.net/mhia261/10-commandments-of-computer-ethics-with-example

Techspirited. (2020). Ten Commandments of Computer Ethics You Should Follow Without Fail. https://techspirited.com/ten-commandments-of-computer-ethics

Upadhyay, I. (2020). Authentication and Authorization: An Easy 2 Step Guide. https://www.jigsawacademy.com/blogs/cyber-security/authentication-and-authorization/

Wang, G. (2014). Thou shalt not use a computer to bear false witness. https://prezi.com/7fuoghmiyd8t/thou-shalt-not-use-a-computer-to-bear-false-witness/